



SPAM & MALWARE PROTECTION

Protection efficace contre le pourriel et les logiciels malveillants grâce à un système de filtrage à plusieurs niveaux, entièrement automatisé

Représentant plus de 50 % de tout le trafic courriel, le pourriel est la méthode la plus intrusive que les cybercriminels utilisent pour introduire des logiciels malveillants et des virus dans les systèmes d'entreprise. En plus du risque d'infection par rançongiciel, logiciel espion ou cryptomineur, des flux de travail importants peuvent aussi être interrompus par l'afflux agaçant de courriels indésirables. Un système de filtrage à plusieurs niveaux est indispensable si vous voulez empêcher les courriels de pourriel et d'hameçonnage d'atteindre vos boîtes de réception et de perturber les opérations.

Vos boîtes aux lettres méritent les filtres les plus robustes



Détection du pourriel à plusieurs niveaux et niveaux de filtres dynamiques



Détection dynamique des éclosions de virus.



Protection contre les attaques DOS à grande échelle et les attaques ciblées de type « mail bombing ».

COMMENT LA PROTECTION CONTRE LE POURRIEL ET LES LOGICIELS MALVEILLANTS VOUS AIDE-T-ELLE À SÉCURISER VOTRE ENVIRONNEMENT DE COURRIEL?



Meilleurs taux de détection du pourriel (99,9 %) et des virus (99,99 %) sur le marché.



Maximisation de la sécurité selon les besoins spécifiques d'un tenant grâce à la création de règles avancées dans le filtre de conformité.



Les courriels sortants sont analysés pour détecter le pourriel et les virus.



Communications courriel entrantes et sortantes sécuritaires.



SPAM & MALWARE PROTECTION

MÉCANISMES D'ANALYSE PRÉCIS ET FILTRES FIABLES :

Filtre d'hameçonnage: Le suivi des liens (link tracking) et d'autres mécanismes protègent efficacement contre les courriels d'hameçonnage. Entre autres, les commandes de scripts malveillants rechargeables sont détectées. Cela permet, par exemple, de détecter des téléchargements furtifs (drive-by downloads) dangereux.

Filtre « infomail » : Les infolettres non classées comme pourriel et d'autres courriels d'information qui interrompent inutilement le travail sont filtrés et conservés pour récupération ultérieure. Ils sont listés dans le rapport de quarantaine individuel et peuvent être livrés et ajoutés à la liste d'autorisation en un clic au besoin.

Suivi des liens : Les courriels entrants et sortants sont automatiquement analysés pour détecter les URL malveillantes.

Mise à jour automatique des signatures virales : Les filtres antimaliçieux sont constamment mis à jour et demeurent à jour. Entre autres, l'entreprise utilise ses propres scanners spécialisés dans les maliçieux propagés par courriel.

Filtrage sortant : Les courriels sortants sont vérifiés pour le pourriel et les virus afin d'éviter que le client n'envoie ou ne transfère involontairement des maliçieux et du pourriel.

Gestion des avis de non-remise : Seuls les avis de non-remise légitimes atteignent le destinataire dans le trafic entrant; les avis générés en réponse à du pourriel avec des adresses d'expéditeur falsifiées sont filtrés de façon fiable.

Filtre de contenu pour les pièces jointes : Les pièces jointes indésirables peuvent être rejetées ou déplacées en quarantaine.

Détection dynamique des éclosions de virus : Les nouveaux virus, y compris ceux auparavant inconnus, sont bloqués par le système d'alerte précoce. Proofpoint analyse en continu les courriels entrants sur des comptes « honeypot » (des adresses courriel dont le seul but est de recevoir du pourriel) afin de repérer des pièces jointes, liens, expéditeurs ou contenus inhabituels. La génération de signatures à partir de ces observations se fait avec un temps de réaction très court (habituellement < 5 minutes).

Moins de 0,00015 de faux positifs : Le nombre de courriels légitimes classés par erreur comme pourriel est inférieur à 0,00015.

GESTION SIMPLE ET RESPECT DES POLITIQUES DE CONFORMITÉ

Rapport de quarantaine à des intervalles configurables : Les utilisateurs peuvent adapter la fréquence de livraison de leurs rapports de quarantaine à leurs méthodes de travail et les planifier à des heures précises, même plusieurs fois par jour.

Libération en un clic : Les courriels en quarantaine peuvent être livrés à partir du rapport de quarantaine en un clic, qu'il s'agisse de pourriel présumé ou de courriels d'information.

Bonne visibilité grâce au blocage : La grande majorité des courriels de pourriel sont bloqués directement. Les utilisateurs obtiennent ainsi un aperçu rapide des courriels actuellement en quarantaine.

Allège la charge du serveur de messagerie : La protection contre le pourriel et les logiciels malveillants ne laisse passer que les messages valides, ce qui améliore considérablement la performance du serveur de messagerie du client.